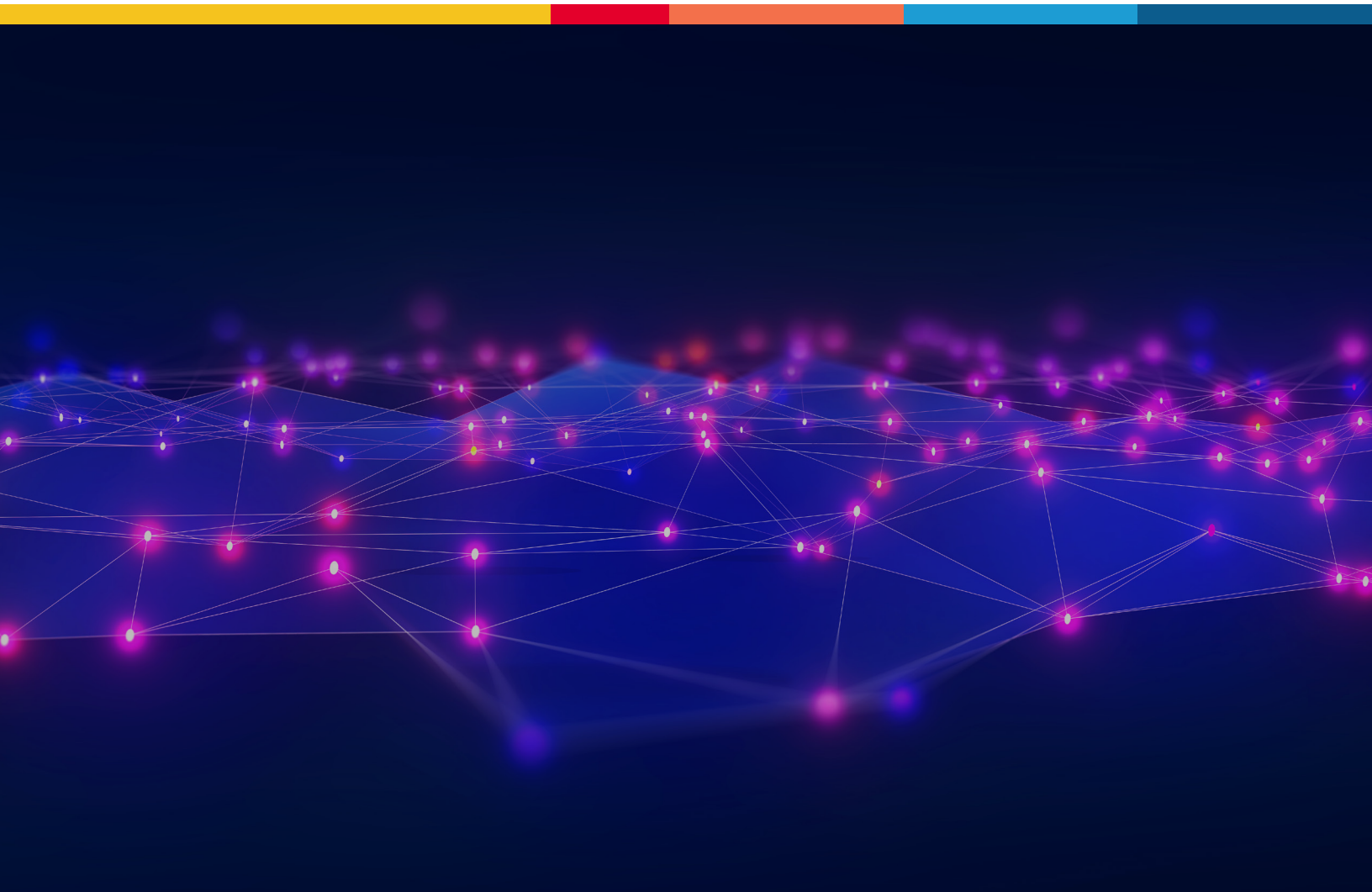
SOLUTION OVERVIEW

Securing GraphQL APIs with BIG-IP Advanced WAF

As GraphQL continues to grow in popularity, it has also captured the attention of cyber adversaries. Discover how F5 BIG-IP Advanced WAF natively secures GraphQL application programming interfaces (APIs), applying attack signatures, eliminating malicious exploits, and defending against DoS attacks.



KEY BENEFITS

Stop false positives
End false positives caused by attack signatures being applied against wrong parts of the GraphQL request.

Eliminate DoS attacks
Maximum structure depth configuration in content profiles stops DoS attacks caused by recursive queries.

Alleviate malicious exploits
Defining maximum batched queries in one HTTP request reduces chances for malicious exploits and attacks.

Address volumetric DoS attacks
Behavioral DoS and machine learning deliver precise L7 DoS detection and mitigation.

Limit API risk exposure
Prevent attackers from gaining an advantage by learning about the API structure.

State of the APIs

The human body is made up of many components, including tissues and organs. Connective tissue supports, protects, and provides a structure for other tissues and organs. Connective tissue in the human body can either be solid and strong or fluid and flexible.

Similarly, the digital world is made up of many components, not the least of which are applications and the data that serves them. What bonds applications and data can be called digital connective tissue, similar to the connective tissue in the human body. Digital connective tissue must also be solid and strong or fluid and flexible. One of the core elements of digital connective tissue is application programming interfaces (APIs).

As our personal and business worlds become increasingly digitally driven, APIs are more important than ever. They serve as the essential digital connective tissue that enables us to live our daily lives online. With APIs, we can shop online, make travel arrangements, compare prices, and more. APIs are the cornerstones of modern applications and are ubiquitous in today's digital life. They connect applications and quickly, simply, and securely share data between them.

APIs may also be used to adapt and update older, classic applications to support newer, more modular languages, tools, and platforms. APIs and the data they share make up most of today's web traffic, regardless of whether the traffic is considered "good" or "bad."

GraphQL

A new API technology that continues to gain traction is GraphQL. Internally developed by Facebook in 2012, GraphQL is now a part of the Linux Foundation. It is an API query language that fulfills queries with existing data, effectively describing the API data. It enables a query for specific data within APIs and provides only the data required and no more, making the results calculable.

GraphQL allows applications to control the data that is requested and received. It can improve the speed and stability of applications, even over slow connections, because it only retrieves the requested data and nothing more.

THE GROWTH AND ACCEPTANCE OF GRAPHQL HAS CAPTURED THE ATTENTION OF ATTACKERS.

GraphQL is quickly overcoming the significant challenges present in REST and SOAP APIs. Typically, with REST or SOAP APIs, there is a need to parse the returned data. The code to parse the data needs to be written manually based on the code and APIs. With GraphQL APIs, this need for manually written parsing codes is eliminated. GraphQL queries an API as well as the connections between APIs and resources. GraphQL can be added to existing APIs without any negative impact, making older APIs run more efficiently. GraphQL APIs require

KEY FEATURES

Native parsing of GraphQL traffic
Allows BIG-IP Advanced WAF attack signatures to be applied against GraphQL traffic

Appropriate attack signature application
Detects attacks in appropriate segments of a payload and runs attack signatures on those values.

Policy templates and content profiles
Enables creation of a GraphQL policy template and content profile as part of application security policy.

Eliminate recursive queries
Configuring maximum structure depth in content profiles helps stop DoS attacks.

Maximum batched queries
Limiting number of different GraphQL queries in a single HTTP request reduces the chance of malicious exploits.

Introspection query enforcement
Restricts attackers' understanding of API structure that aids in more successful application breaches.

a single request to gather all the data that an application requests and needs. They can also be created uniformly across an application and are not tied to a specific database or storage engine. Because of these and other benefits, GraphQL is simpler, quicker, and more efficient than REST or SOAP APIs.

With its growing popularity, GraphQL has become a target for attackers. The widespread use of APIs has made them one of the fastest growing and most frequently exploited attack vectors. Exploiting an API enables attackers a quick, simple entry point to compromise an application and manipulate or steal sensitive data. Attackers are already searching for vulnerabilities in the GraphQL ecosystem and are actively developing tools to exploit them. Attack techniques used against GraphQL APIs include SQL injections. New attacks also attempt to leverage the GraphQL specification to reveal data about the API and use it for malicious purposes. There have also been instances of denial-of-service (DoS) attacks leveraging GraphQL-based APIs, which can quickly drain server resources.

BIG-IP Advanced WAF and GraphQL Security

F5® BIG-IP® Advanced WAF® is designed to natively secure GraphQL APIs. F5 has developed native parsing of GraphQL traffic to allow Advanced WAF attack signatures to be applied. This approach detects attacks in the appropriate segments of a payload and runs the signatures on those values. This will also stop false positives due to attack signatures running on the wrong parts of GraphQL requests.

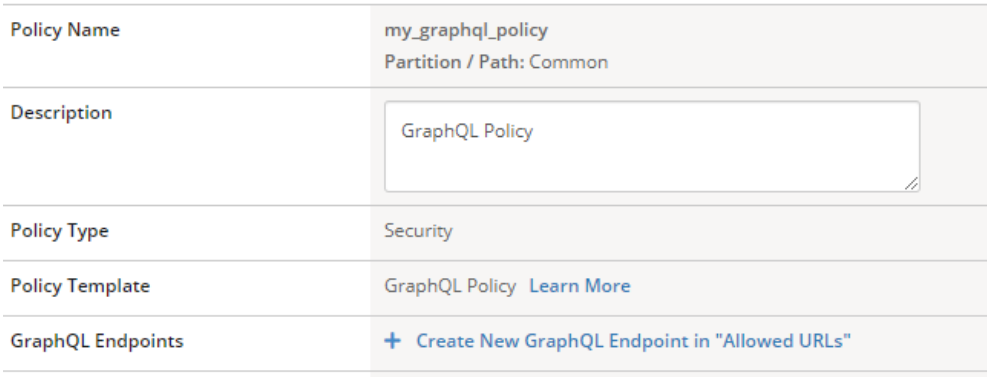


Figure 1: F5 natively supports security for GraphQL APIs.

F5 BIG-IP ADVANCED WAF NATIVELY SECURES GRAPHQL APIS, APPLYING ATTACK SIGNATURES, ELIMINATING MALICIOUS EXPLOITS, AND DEFENDING AGAINST DOS ATTACKS.

F5 creates a GraphQL policy template and content profile as part of its application security policy. An organization can configure the total length and value length of parameters in the content profile, setting limits according to their policy. They can also configure the maximum structure depth to eliminate recursive GraphQL queries that can lead to a DoS attack. Maximum batched queries can also be defined, limiting the number of different GraphQL queries in a single HTTP request and reducing the risk of malicious exploitation.

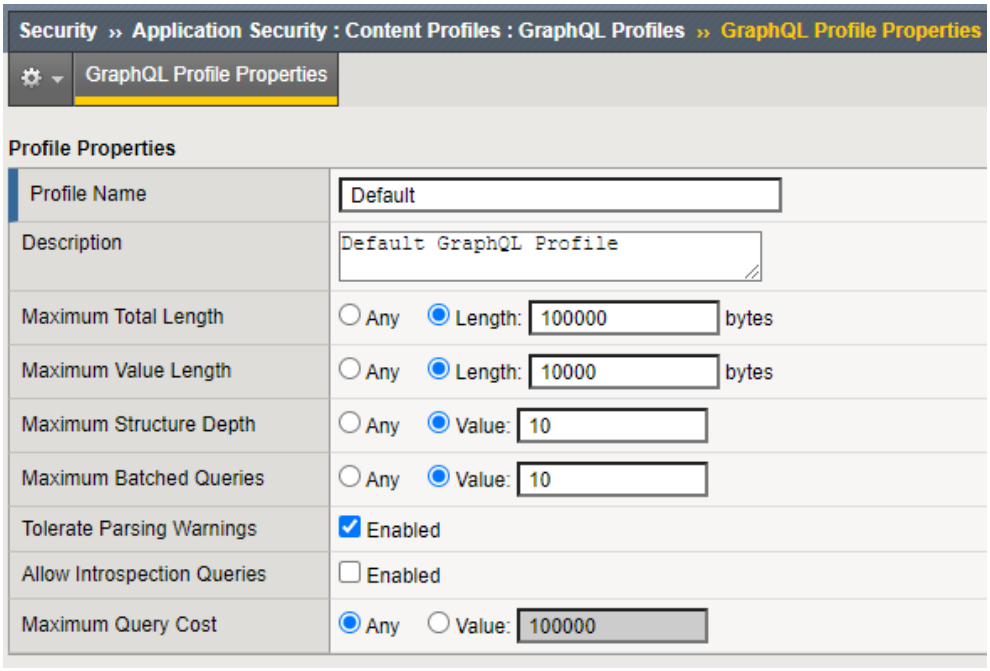


Figure 2: F5 creates the GraphQL policy template and content profile as a part of the application security policy.

Introspection queries can also be enforced to prevent attackers from using them to understand the API structure and potentially breach an application. BIG-IP Advanced WAF also includes support for declarative policy configuration and protects against volumetric DoS attacks through its behavioral DoS capabilities. In addition, BIG-IP Advanced WAF's DataSafe feature allows for the filtering of responses.

Conclusion

GraphQL is simplifying the evolution of APIs and is on track to becoming one of the leading standards for APIs. It offers new ways to create and manage APIs, enhances application modernization, and supports ongoing digital transformation.

However, as with any new technology, attackers are planning and devising new, more sophisticated threats to exploit any vulnerabilities in security. GraphQL is no exception.

Avoid being caught off guard. Deploy BIG-IP Advanced WAF to protect and secure your GraphQL, REST, and SOAP APIs, as well as your essential applications and critical data.

To learn more about protecting your GraphQL APIs with F5 BIG-IP Advanced WAF, contact F5 Sales.